CentralIT
Tecnologia em Negócios

COMPROMISSO COM A SEGURANÇA DA INFORMAÇÃO

Versão 1.0
Maio 2024

Sumário

1 OBJETIVO

A Central IT estabelece uma política abrangente para a gestão da segurança da informação, delineando responsabilidades, padrões e procedimentos para mitigar os riscos relacionados à segurança da informação.

Atualmente a posse da informação significa enorme oportunidade de negócios, principalmente para uma empresa como a Central IT, que possui na informação o seu principal patrimônio.

Informação é um ativo que, como qualquer outro, tem muito valor para a organização e consequentemente necessita ser adequadamente protegido.

A informação pode ser disponibilizada de várias formas, podendo ser impressa ou escrita em papéis, armazenada eletronicamente, transmitida por correio ou por meios eletrônicos ou apresentar-se através de conversação. Seja qual for o meio pelo qual a informação é distribuída, partilhada ou armazenada, a mesma sempre requer proteções apropriadas.

A Segurança da Informação tem a função de proteger a informação de uma série de ameaças com o objetivo de zelar pela continuidade dos negócios, minimizar prejuízos e maximizar o retorno de investimentos e oportunidades de negócios. Desta forma, a segurança da informação torna-se responsável pela preservação dos seguintes aspectos da informação:

a) Confidencialidade: assegura que a informação permaneça acessível apenas a quem de direito;

b) Integridade: protege a exatidão e a totalidade da informação e das possíveis formas de processamento desta;

c) Disponibilidade: assegura que usuários autorizados tenham acesso à informação e aos ativos associados a ela quando necessário.

Fonte: ABNT NBR ISO/IEC 27002:2022

Para que a Segurança da Informação seja eficaz, depende do planejamento, análise e implementação de uma série de controles, compostos por políticas, práticas, procedimentos, estruturas organizacionais ou mecanismos eletrônicos e cada um tem responsabilidade internamente.

Neste documento, serão abordados os seguintes capítulos:

1. Capítulo 2 - Governança e Gestão da Segurança da Informação:
    a. Estabelece a base para a segurança da informação na organização.
    b. Inclui estrutura da gestão, política de segurança e gerenciamento de riscos.
2. Capítulo 3 - Segurança dos Colaboradores:
    a. Garante que os colaboradores estejam conscientes dos riscos e aptos a agir de forma segura.
    b. Abrange conscientização, treinamento, seleção e segurança de pessoal.
3. Capítulo 4 - Segurança Física:
    a. Protege os ativos físicos contra acessos não autorizados, danos e perda de dados.
    b. Inclui controle de acesso físico, segurança de equipamentos e continuidade de negócios.
4. Capítulo 5 - Segurança Tecnológica:
    a. Protege sistemas e dados contra-ataques cibernéticos, malware e outras ameaças tecnológicas.
    b. Abrange segurança de rede, recurso de software, controle de acesso, criptografia e sincronização de relógio.

1.1 Importância da informação

De forma crescente os sistemas de informações têm sido expostos a uma série de ameaças, dentre as quais podemos citar como exemplos, fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundações.

Desta forma podemos concluir que, nos parâmetros atuais, a segurança da informação é vital para a continuidade do negócio de qualquer organização, bem como dependente da participação ativa de todos os seus funcionários, seja em sua implementação e manutenção continua.

Todas as informações criadas, manuseadas, armazenadas, transportadas ou descartadas pelos colaboradores no exercício de atividades, sejam de propriedade da Central IT ou de terceiros, como fornecedores, clientes, parceiros e colaboradores, são de responsabilidade da Central IT. Essas informações devem ser protegidas adequadamente e não devem ser divulgadas, salvo quando permitido.

1.2 A política de Segurança da Informação, Segurança Cibernética e Proteção à Privacidade

Este documento constitui um instrumento essencial que oferece diretrizes detalhadas para orientar a organização no planejamento, definição e implementação de mecanismos abrangentes, como normas, procedimentos, padrões, controles e outros dispositivos. Esses recursos foram concebidos para respaldar e aprimorar as atividades relacionadas à segurança da informação, segurança cibernética e proteção da privacidade. Eles são especialmente direcionados para as áreas identificadas como de maior risco para os processos de negócios da organização, garantindo uma abordagem proativa e eficaz para mitigar possíveis ameaças e vulnerabilidades.

A política de Segurança da Informação, Segurança Cibernética e Proteção à Privacidade da Central IT foi definida com base nas necessidades de segurança exigidas pelos negócios da empresa, conforme relacionado:

- Documentada adequadamente e seguida por todas as pessoas envolvidas direta ou indiretamente na execução e condução dos processos de negócios da organização e/ou atividades que envolvam o tratamento de dados pessoais;
- Revisada conforme necessário para garantir sua conformidade com as diversas mudanças enfrentadas pela organização.
- Monitorada pelos funcionários da organização, sendo eles responsáveis por relatar de forma íntegra quaisquer incidentes ocorridos.

A avaliação da eficácia dos controles de segurança da informação será conduzida através de relatórios de auditoria interna ou análises críticas de vulnerabilidades em recursos. Esse processo ocorrerá, no mínimo, anualmente e sempre que necessário.

1.3 Partes Interessadas

Este documento foi elaborado para atender às necessidades e expectativas das partes interessadas, que incluem a Alta Direção, Superintendentes, Acionistas, Colaboradores, Clientes, Fornecedores, Parceiros, Órgãos Públicos e Privados. A Central IT se compromete a satisfazer essas expectativas e necessidades em relação ao sigilo, confidencialidade e integridade das informações, por meio da aplicação de sua Política de Segurança da Informação, Segurança Cibernética e Proteção à Privacidade.

A criação deste documento tem como objetivo estabelecer uma política abrangente, abordando os pontos sensíveis que são tratados em tópicos e documentos específicos, os quais possuem níveis de sensibilidade definidos.

1.4 Uso de recursos corporativos

É importante lembrar também que todo uso de recursos de tecnologia da informação disponibilizados pela Central IT tais como e-mail, sistemas, Internet, bem como fornecidos por terceiros, no uso e atribuições da Central IT, devem ser utilizados estritamente para uso profissional e no interesse da Central IT.

Serão considerados fins indevidos: fraudes, invasão, jogos, uso de Proxy não autorizado, acesso não autorizado, personificação, falsa identidade, obtenção de senhas e dados privativos, perseguição, ameaças, downloads não autorizados, distribuição de códigos maliciosos, vírus, acesso e disseminação de materiais pornográficos, ofensivos, difamatórios, discriminatórios, preconceituosos e atentatórios à moral e aos bons costumes, instalação de softwares piratas, veiculação de opiniões político-partidárias ou religiosas, conteúdos ilegais de incitação à violência, que não respeitem os direitos autorais ou objetivos comerciais particulares; spam; distribuição de correntes de mensagens eletrônicas, vazamentos intencionais de dados, ações que comprometam a integridade, a confidencialidade ou a disponibilidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pela Central IT, cometimento de crimes ou que venham a prejudicar, mesmo de forma não intencional, outros colaboradores, pessoas e instituições vinculadas à prestação de serviços ou recursos da Central IT.

As informações de caráter de identificação pessoal ou qualquer outro dado sensível particular de colaborador, cliente ou parte interessada, tem respeitada sua privacidade conforme requerido por legislação e regulamentação.

1.5 Palavra do Presidente do Conselho de Acionistas Central IT

É obrigação de colaboradores e parceiros preservar a “confidencialidade das informações” de forma que se garanta o sigilo quando for necessário, “a integridade” de maneira que as informações estejam sempre corretas e a “disponibilidade” para que

sempre que um usuário precise de uma informação, os sistemas estejam em perfeitas condições para atendê-lo.

Para isto a Central IT investe e prove recursos, governança corporativa, soluções e padrões tecnológicos a fim de aumentar e melhorar a produtividade individual e coletiva de seus colaboradores. Esta diretriz foi elaborada com objetivo de garantir a segurança da informação e a proteção de dados pessoais e atende aos pré-requisitos do bom uso dos recursos computacionais da Central IT.

Conto com a participação de todos os nossos colaboradores na preservação e disseminação das diretrizes contidas neste documento, para que possamos entregar cada vez mais confiabilidade e credibilidade aos nossos clientes.

Carlos Freitas

Presidente do Conselho de Acionistas

2 GOVERNANÇA E GESTÃO DA SEGURANÇA DA INFORMAÇÃO

2.1 Responsabilidades sobre Segurança da Informação e Proteção de Dados Pessoais

2.1.1 Responsabilidades da Alta Direção

As responsabilidades da Alta Direção são definidas e revisadas regularmente pelo Conselho de Acionistas, incluindo o cumprimento das seguintes atribuições:

a) Definição e comunicação dos objetivos estratégicos relacionados à segurança da informação e conformidade com as normativas de proteção de dados, garantindo a disseminação dessa cultura por toda a organização;
b) Atribuir responsabilidades específicas para a gestão de segurança da informação.
c) Garantia da disponibilização dos recursos necessários para implementar e fortalecer os controles de segurança;
d) Acompanhamento e avaliação constante da implementação de soluções de segurança, assegurando a eficácia e relevância dessas medidas diante das necessidades em evolução;

2.1.2 Gestor de Segurança da Informação

A função de gestor de segurança da informação é revista sempre que necessário pela alta direção e visa a execução das seguintes tarefas:

a) Planejamento e condução de conscientização periódicos com o objetivo de disseminar a cultura de segurança dentro da Central IT, bem como de comunicar as atualizações eventualmente efetuadas na Política de Segurança da Informação, Segurança Cibernética e Proteção à Privacidade;
b) Apoio à equipe de infraestrutura na identificação dos ativos da Central IT e os responsáveis;
c) Monitoração do atendimento aos padrões, diretrizes e procedimentos vigentes em conjunto com a qualidade;
d) Acompanhamento das vulnerabilidades, dos pontos fracos existentes, dos riscos e ameaças eventualmente identificadas em auditorias de segurança, em conjunto com a qualidade;
e) Implementação de controles com o auxílio dos Gerentes e coordenadores de cada área, em conjunto com a qualidade;
f) Acompanhamento da implementação de soluções de segurança;
g) Apoio à qualidade na condução de revisões periódicas de segurança a fim de garantir que a política esteja sendo adequadamente seguida.

2.1.3 Usuário

Entende-se por Usuário qualquer pessoa que utiliza os sistemas, aplicativos ou recursos de tecnologia da informação fornecidos pela Central IT para realizar suas tarefas ou atividades relacionadas ao trabalho. Isso inclui funcionários, contratados, clientes ou qualquer outra pessoa autorizada a acessar e utilizar os recursos de TI da Central IT, para cumprir suas funções.

As responsabilidades dos usuários são:

a) Proteger a integridade, disponibilidade e confidencialidade dos ativos associados;
b) Reportar os incidentes e as fragilidades de segurança da informação e de privacidade e proteção de dados pessoais;

c) Seguir diretrizes, normas e políticas definidas de segurança de informação e de privacidade e proteção de dados pessoais.

2.1.4 Encarregado pelo Tratamento de Dados Pessoais

O Encarregado é a pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.
Dentre as responsabilidades do Encarregado, estão:

a) Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
b) Receber comunicações da Autoridade Nacional de Proteção de Dados (ANPD) e adotar providências;
c) Orientar os colaboradores e os contratados da organização a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
d) Atender às atribuições determinadas pelo controlador, pela ANPD e/ou estabelecidas em normas complementares;
e) Apoiar a gestão dos incidentes que envolvam dados pessoais, garantindo o tratamento adequado e comunicando os envolvidos, conforme legislação aplicável;
f) Identificar e avaliar as ameaças à privacidade e proteção de dados, bem como propor, e quando aprovado, apoiar a implantação de medidas corretivas para as tratativas dos riscos;
g) Apoiar o Comitê de Segurança da Informação e Proteção de Dados Pessoais em suas deliberações;
h) Tomar as ações cabíveis para se fazer cumprir os termos desta política.

2.1.5 Comitê de Segurança da Informação e Proteção de Dados Pessoais

O Comitê é composto por um grupo multidisciplinar da organização e é focado nos aspectos relacionados à privacidade e proteção de dados, além de prestar apoio ao Encarregado em suas atribuições.

Dentre as responsabilidades do Comitê, estão:

a) Analisar, revisar e aprovar políticas, normas, procedimentos etc., relacionados à privacidade e proteção de dados pessoais;
b) Auxiliar na implementação das mudanças a fim de mitigar os riscos relacionados à privacidade e proteção de dados;
c) Auxiliar na implementação de medidas de segurança desde a fase de planejamento de projetos, sistemas, processos, procedimentos etc.;
d) Auxiliar na manutenção da conformidade com as legislações através de métricas, controles, auditorias periódicas entre outros;
e) Zelar para que tratamento de dados pessoais seja realizado em conformidade com esta política e a legislação vigente;
f) Promover a divulgação desta política e tomar as ações necessárias para disseminar a cultura de privacidade e proteção de dados pessoais na organização;
g) Auxiliar na conscientização dos colaboradores sobre as políticas, normas, procedimentos etc., referentes à privacidade e proteção de dados pessoais;
h) Realizar reuniões periódicas.

2.2 Tratamento de dados pessoais

A Central IT visa garantir a gestão efetiva de todos os aspectos relacionados à privacidade e proteção de dados pessoais e dos direitos dos seus respectivos titulares, provendo suporte as operações do negócio minimizando riscos e eventuais impactos à organização.

Nas atividades de tratamento~~s~~ de dados pessoais, são diretrizes da Central IT:

a) Expressar, de maneira clara, objetiva e adequada ao contexto, como os dados pessoais serão tratados para o titular, antes da primeira coleta ou utilização.
b) Fornecer aos titulares dos dados pessoais, informações claras e de fácil acesso, conforme legislação vigente;
c) Garantir que as atividades de tratamento de dados pessoais estejam em conformidade com a legislação vigente aplicável;
d) Realizar a coleta de dados pessoais de acordo com a legislação vigente e com os objetivos especificados;
e) Reter dados pessoais apenas pelo tempo necessário para o cumprimento dos propósitos declarados e/ou para o cumprimento de obrigações legais;

f) Prezar pela qualidade dos dados pessoais tratados;
g) Tratar os incidentes que envolvam vazamentos de dados pessoais, garantindo que sejam devidamente registrados, classificados, investigados, corrigidos e documentados;
h) Disponibilizar políticas, normas, procedimentos, orientações e/ou práticas relacionadas à privacidade e proteção de dados pessoais a todas as partes interessadas e autorizadas, tais como: colaboradores, parceiros, terceiros e/ou clientes, quando aplicável;
i) Adotar medidas técnicas e administrativas com o intuito a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
j) Promover treinamentos, palestras e/ou workshops, objetivando o fortalecimento da cultura de privacidade e proteção de dados na organização;
k) Melhorar continuamente os processos/atividades relacionados à privacidade e proteção de dados pessoais;
l) Zelar pela não discriminação dos indivíduos no tratamento de dados pessoais;
m) Comunicar aos titulares quando ocorrerem alterações significativas no tratamento dos seus dados pessoais.

2.3 Classificação da Informação

O processo de classificação e rotulagem de informações é fundamental para proteger os ativos de informação da Central IT, garantindo que apenas pessoas autorizadas tenham acesso a informações confidenciais. Isso assegura a confidencialidade, integridade e disponibilidade dos dados.

Nível	Descrição	Quem pode classificar	Quem acessa	Rótulo
Pública	Documentos e informações que o acesso é permitido a todas as pessoas.	Controladoria e Qualidade	Qualquer pessoa, interna ou externa, à Central IT	**Público**
Acesso Interno	Documentos e informações que contém procedimentos e modelos utilizados pela Central IT.	Controladoria e Qualidade	Todos os colaboradores internos da Central IT	**Interno**
Restrita	Documentos que contenham informações de caráter pessoal, análises e tratativas com clientes, de relacionamento com fornecedores ou que sua divulgação interna possa causar prejuízos à Central IT no que se refere à sua reputação ou harmonia de funcionamento.	Controladoria e Qualidade	Apenas colaboradores internos da área, ou grupos de trabalho, onde é executado o processo, inclusive pessoas às quais o gestor da informação der acesso (inclusive clientes e fornecedores), assim como Superintendentes e Diretores.	**Restrito**
Confidencial	Documentos que contenham informações estratégicas para a Central IT, incluindo prospecção de novos clientes ou que possam causar danos à imagem da Central IT ou prejuízos financeiros	Controladoria e Qualidade	Apenas pessoas indicadas pelo gestor da informação.	**Confidencial**

Tabela 01 – Quadro para Classificação da Informação

* As informações compartilhadas com fornecedores, clientes e outros agentes externos à Central IT, deverão ter o devido controle para que se evite que o agente externo divulgue uma informação indevidamente. No caso das informações produzidas pelo agente externo, será dado o tratamento orientado pelo agente ou a inclusão de maior grau de restrição de acesso, caso o gestor da informação da Central IT avalie como necessário. O tratamento dado pela Central IT às informações recebidas de agentes externos nunca poderá ser de maior grau de ostensividade do que o informado pelo agente externo.

2.4 Transferências de informações

2.4.1 Canais de comunicação eletrônica

As informações da organização devem ser trocadas por meio dos seguintes canais de comunicação eletrônica: e-mail, office 365 corporativo, transferência de dados via ftp, telefones corporativos, site corporativos internos/externos.

2.4.2 Relações com partes externas

Partes externas incluem os diversos fornecedores de serviços, empresas de manutenção de hardware e software, empresas que gerenciam transações, processamentos de dados ou clientes.

Caso haja necessidade de trocas de dados confidenciais e sigilosos, antes de qualquer procedimento que vise o câmbio dessas informações e/ou softwares com qualquer parte externa, um contrato deve ser formalizado. Todos os trâmites são de responsabilidade do gestor do departamento contratante.

O contrato poderá ser formalizado fisicamente ou em formato eletrônico e deve conter cláusulas que estejam de acordo com a avaliação de riscos, incluindo, no mínimo:

- O método de identificação do terceiro;
- As autorizações para acesso às informações;
- A garantia de não repúdio;
- As normas técnicas para transferência de dados;
- A resposta a incidentes;
- Os rótulos e a gestão de informações confidenciais ou restritas;
- Os direitos autorais;
- Sigilo e confidencialidade das informações acessadas durante e após o contrato.

Os contratos com as partes externas precisam ser definidos considerando:

- A anuência de requisitos de segurança da informação da Central IT por intermédio de, no mínimo, uma das opções: Assinatura do TERMO DE CIÊNCIA DA POLÍTICA DE SEGURANÇA DO FORNECEDOR, a inclusão de cláusulas de sigilo ou confidencialidade no contrato firmado ou Assinatura do termo de confidencialidade padrão Central IT;

- Seguir os princípios e regras básicas estabelecidas no documento POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA FORNECEDORES.
- O acesso fornecido será monitorado por intermédio dos controles de redes vigentes.

2.5 Correio eletrônico

O uso de correio eletrônico deve cumprir diretrizes, conforme o item 1.4 somando-se as ponderações abaixo:

a) Uso do correio eletrônico como uma ferramenta de comunicação da Central IT, não devendo ser utilizada para assuntos pessoais;
b) Tráfego inadequado de informações confidenciais ou restritas.
c) Os e-mails corporativos são considerados propriedade da empresa, sendo direito resguardado pelo contrato de trabalho, acordo de confidencialidade e cláusulas de direito de propriedade intelectual.

2.6 Gerenciamento de Acesso

2.6.1 Política de senha

As senhas de acesso aos sistemas e a contas de e-mails são pessoais, confidenciais, intransferíveis e de total responsabilidade do colaborador. Os colaboradores e terceiros são responsáveis por todas as ações feitas sob seu acesso e responderão civil e criminalmente por quaisquer abusos cometidos neste contexto.

2.6.2 Registro de usuários

O registro de novos colaboradores deve ser realizado pelo Departamento Pessoal, enquanto a disponibilização dos acessos necessários à rede corporativa é responsabilidade do suporte interno (infraestrutura de TI) da Central IT. Este processo será conduzido em conformidade com os princípios do Gerenciamento de Acessos, conforme descrito na ISO 27001:2022 e procedimentos internos da Central IT, que estabelece diretrizes para o registro e manutenção dos acessos corporativos.

Adicionalmente, é fundamental que os usuários sigam as orientações de segurança da informação ao definir suas senhas, garantindo que sejam fortes e seguras. Recomenda-se o uso de uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais. Por exemplo, uma senha forte pode ser "P@ssw0rd!". Além disso, as senhas devem ser trocadas periodicamente conforme as políticas estabelecidas pela empresa, que podem ser configuradas através de uma Política de Grupo (GPO, Group Policy Object) no ambiente de rede.

2.6.3 Exclusão de usuários

A exclusão dos acessos se dará após o departamento pessoal promover o desligamento do colaborador no sistema correspondente.

2.6.4 Gerenciamentos de acessos de terceiros

Os prestadores de serviços, incluindo os terceirizados, possuem em seus contratos de trabalho as instruções relacionadas às necessidades de acessos, que devem ser seguidos igualmente às cláusulas constantes nos termos de compromisso de segurança, aplicados a todos os funcionários.

2.7 Segurança em Nuvem

A Central IT estabelece as diretrizes para o uso seguro dos serviços em nuvem, visando prevenir incidentes que possam comprometer as operações de negócio e ameaçar a segurança da informação. Essas diretrizes estão de acordo com a política POLÍTICA DE USO DE SERVIÇOS EM NUVEM, que define os padrões e práticas aceitáveis para o emprego seguro desses serviços.

As ações realizadas na utilização de serviços em nuvem devem seguir os princípios estabelecidos na política mencionada, garantindo a integridade, confidencialidade e disponibilidade das informações. Além disso, devem estar alinhadas aos objetivos estratégicos da organização e às normativas de segurança estabelecidas.

É responsabilidade de todos os colaboradores compreender e aderir à política de uso de serviços em nuvem, buscando a mitigação de riscos e o fortalecimento da postura de

segurança da informação da Central IT. A atualização e revisão periódica desta política são essenciais para assegurar a conformidade contínua com as melhores práticas de segurança e para adaptar-se a possíveis evoluções no cenário de segurança da informação e tecnologia em nuvem.

2.8 Resposta a Incidentes de Segurança

A resposta a incidentes de segurança deve abranger a contenção dos sistemas afetados, coleta rápida de evidências, escalonamento com gestão de crises, registro de atividades para análise, comunicação do incidente, coordenação com partes internas e externas, encerramento do incidente, análise pós-incidente para identificar a causa-raiz, e gestão de vulnerabilidades em sistemas de informação.

Assim que o incidente for detectado, deve ser relatado o mais breve possível e formalizado por meio de procedimento específico chamado INCIDENTES E REQUISIÇÃO DE SERVIÇOS.

2.9 Prontidão de TIC para continuidade de Negócio

Com o propósito de estabelecer diretrizes e objetivos para garantir a prontidão da Tecnologia da Informação e Comunicação (TIC) em situações de continuidade de negócio na Central IT, foi desenvolvido o Plano de Continuidade de Negócio (PCN), identificado como PLANO DE CONTINUIDADE DE NEGÓCIO - PCN. Este plano delineia os procedimentos e estratégias a serem seguidos em casos de interrupções não planejadas ou eventos que possam afetar a operação normal da empresa.

As medidas descritas neste plano têm como objetivo principal preservar a funcionalidade dos sistemas de TIC essenciais para as operações, assegurando a resiliência diante de possíveis interrupções. O foco está em garantir a disponibilidade, integridade e confidencialidade dos dados críticos, ao mesmo tempo em que se busca minimizar o tempo de inatividade e seus impactos nos serviços prestados pela organização.

A execução eficiente deste plano é crucial para garantir a rápida recuperação e retomada das atividades normais após eventos adversos. Este documento serve como um guia abrangente para assegurar que a TIC da Central IT esteja preparada para enfrentar e

superar interrupções imprevistas, garantindo a resiliência e a continuidade das operações mesmo em situações adversas.

2.10 Gerenciamento de Risco

Com o objetivo de mitigar os impactos de eventos imprevisíveis, a Central IT conduz a gestão de riscos organizacionais em suas áreas internas e contratos. Este processo identifica e mapeia as vulnerabilidades em cada área e contrato, que podem se manifestar como riscos potenciais.

Os riscos identificados são analisados e classificados quanto à sua probabilidade e impacto, permitindo a avaliação do seu valor e a decisão de aceitação ou não. Durante essa análise, são também identificados os controles corporativos necessários, o tipo de tratamento adequado e os planos de ação correspondentes.

É realizado anualmente um contato com as áreas internas e contratos, visando revisar os riscos existentes, encerrar aqueles que não representam mais uma ameaça ativa e incluir novos riscos mapeados ao longo do ano mediante a procedimento formal de Gestão de Riscos.

3 SEGURANÇA DOS COLABORADORES

3.1 Divulgação da Política de Segurança da Informação, Segurança Cibernética e Proteção à Privacidade

A divulgação da Política de Segurança da Informação, Segurança Cibernética e Proteção à Privacidade, está de acordo com os processos já adotados pela Central IT para divulgação de outros documentos e políticas.

Todos os envolvidos na implementação da política, incluindo a alta direção, gerências, funcionários e terceiros, devem entender, conscientizar-se e comprometer-se com o conteúdo da política e de seus adendos, comprovando o atendimento a estes pré-requisitos formalmente, através da assinatura do “Termo de Confidencialidade e Sigilo” e ou do “Contrato Individual Trabalho a Título de Experiência”. Desta forma, o termo em questão faz parte da documentação pessoal exigida pela área de Gestão de Pessoas para cada funcionário, bem como dos contratos exigidos pela Central IT aos terceiros e estagiários sempre que aplicável.

3.2 Capacitação e Conscientização de Pessoal

Com o objetivo de manter os colaboradores e prestadores de serviços (conforme julgue necessário) adequadamente cientes e preocupados com as ameaças à segurança das informações, a Central IT deve conscientizar seus colaboradores, sobre a utilização adequada de procedimentos de segurança, privacidade e proteção de dados.
O planejamento e a condução desta conscientização em questão são de responsabilidade do Gestor de Segurança da Informação, Assessoria Jurídica e Compliance em conjunto com o departamento de Gestão de Pessoas, mediante a treinamento obrigatórios aos colaboradores da organização.

4 SEGURANÇA FÍSICA

4.1 Política de mesa limpa e tela limpa

As informações categorizadas como "Uso interno", "Restrito" e "Confidencial" foram classificadas de acordo com os critérios estabelecidos no documento CLASSIFICAÇÃO E ROTULAÇÃO DA INFORMAÇÃO.

4.1.1 Política de mesa limpa

Caso a pessoa autorizada não estiver no local de trabalho, todos os documentos em papel e todas as mídias de armazenamento de dados classificadas como confidenciais ou restritas devem ser removidas da mesa ou de outros locais (impressoras, copiadoras, etc.) para evitar o acesso não autorizado.
Mesmo em teletrabalho, deve-se ter os devidos cuidados com o vazamento indevido de informações. Esses documentos e mídias devem ser armazenados de forma segura.

4.1.2 Política de tela limpa

Se a pessoa autorizada não estiver em seu posto de trabalho, todas as informações confidenciais ou restritas devem ser removidas da tela e o acesso deve ser bloqueado a todos os sistemas aos quais essa pessoa possui autorização de acesso.
No caso de uma breve ausência (de até 10 minutos), é executada a política de tela limpa, implementada por meio de política de rede com bloqueio da tela, solicitando uma senha.

4.2 Proteção de instalações e equipamentos compartilhados

Os documentos que contêm informações confidenciais ou restritas devem ser removidos imediatamente de impressoras e copiadoras.
As instalações para envio e recepção de correspondências através das recepções são protegidas através de envelopes e classificadas através de protocolo.
O uso não autorizado de impressoras, copiadoras, escâneres e outros equipamentos compartilhados para cópias é controlado através do uso de PIN para liberar cópias e pela localização desses equipamentos em salas fechadas.

4.3 Dispositivos Móveis

Os dispositivos móveis compreendem todos os tipos de computadores portáteis e celulares/smartphones.
Não é permitida a inclusão ou utilização de equipamentos particulares ou de terceiros na rede corporativa da Central IT sem o devido consentimento e autorização prévia da equipe de infraestrutura interna. Caso seja necessário utilizar um equipamento externo, a equipe de infraestrutura deverá disponibilizar um meio seguro que não comprometa a segurança da rede da Central IT. O não cumprimento desta orientação está sujeito a procedimentos administrativos e criminais
De acordo com a regras básicas de utilização, tais equipamentos, somente deverão ser retirados das instalações da empresa após autorização.

4.3.1 Regras básicas de utilização - Segurança de ativos fora das instalações da organização

O colaborador que estiver portando dispositivos móveis, externamente às dependências da empresa, deverá se atentar para as seguintes regras:

a) As atualizações de patches de segurança e proteção contra códigos maliciosos são de responsabilidade da equipe de suporte de infraestrutura interna e deverão ser realizadas em intervalos regulares.
b) O colaborador que fizer uso de dispositivos móveis fora das instalações da empresa será necessário utilizar os meios de armazenamento corporativos (Sharepoint ou outro local definido pela empresa).
c) Recomenda-se não armazenar informações confidencias localmente em dispositivos móveis e/ou externos, como pendrives e HDs externos.
d) O colaborador não deve utilizar redes Wi-Fi públicas abertas para troca de informações sigilosas, confidenciais ou restritas.

Além disso, para garantir a segurança e a integridade das comunicações, recomenda-se o uso de uma conexão VPN (Virtual Private Network) ao acessar recursos da empresa fora de suas instalações físicas. A VPN proporciona uma camada adicional de proteção ao criptografar o tráfego de dados, tornando-o mais seguro contra possíveis interceptações por parte de terceiros.

4.4 Segurança Física

Procedimentos para controles, segurança e prevenção de acesso físico não autorizado são adotados pela Central IT, onde ambientes restritos possuem controle de acesso. Tais procedimentos e controles são usados para proteger áreas como: centros de processamento de dados e salas com equipamentos de comunicação e fornecimento de energia.

4.5 Descarte e Destruição de Equipamentos e Mídias

Os dados e softwares licenciados armazenados em mídias móveis, como CD, DVD, pen drive USB, cartão de memória, e em equipamentos contendo mídias de armazenamento,

como computadores e notebooks, devem ser permanentemente destruídos para evitar qualquer recuperação posterior. Alternativamente, a mídia pode ser fisicamente destruída antes do descarte. O gerenciamento de mídias removíveis é realizado por meio do MANUAL DE GERENCIAMENTO DE MÍDIAS REMOVÍVEIS.

4.5.1 Reutilização de Equipamento

Para situações envolvendo a reutilização de equipamentos, estes serão submetidos a um processo de formatação prévia antes de serem reintegrados ao uso, conforme delineado nas diretrizes interna a ser feita pela equipe de Suporte Infraestrutura Interna Central IT.

5 SEGURANÇA TECNOLÓGICA

5.1 Backup das informações

A política de segurança da informação da Central IT visa proteger os dados da organização, garantindo sua disponibilidade e recuperabilidade em caso de falha de equipamento, destruição intencional de dados ou desastre. O objetivo principal do sistema de backup é gerenciar, em colaboração com os usuários, todas as informações críticas da Central IT que requerem cópias de segurança em fita e disco, definindo o momento de cópia, retenção, recuperação e descarte seguro da informação.

Todos os serviços e servidores em produção da Central IT são submetidos a backups, com especial atenção aos serviços críticos identificados, garantindo a restauração de acordo com as necessidades operacionais. Além disso, é fundamental que as cópias de segurança sejam testadas periodicamente para verificar sua integridade, conforme estipulado na política de backup.

Em caso de implementações e criação de soluções de tecnologia que foram contratadas devem sempre ser informadas a equipe de Suporte a Infraestrutura Interna para que este backup seja inserido na politica de backup.

Para garantir a segurança dos dados, as cópias de segurança são armazenadas em locais externos, distantes e independentes das instalações físicas da organização, assegurando a proteção contra possíveis danos ou perdas.

5.2 Recursos de software

A instalação/atualização/remoção de softwares é de responsabilidade de equipe de suporte interno (infraestrutura de TI) da Central IT. Estes serviços quando necessários devem ser solicitados pelos canais de atendimento corporativo.
É expressamente proibida a remoção de sistemas de detecção, prevenção e eliminação de vírus de equipamentos móveis sem autorização da equipe de suporte interno (infraestrutura de TI) da Central IT.
Todo colaborador, interno ou externo, deve zelar pela segurança cibernética é física corporativa desta forma todo e qualquer aspectos que possa ser classificado como risco deve ser notificado pelos canais competentes e em casos que necessitem investigação, terem registro de incidente de segurança no ITSM Central IT.

5.3 Criptografia

O gerenciamento de chaves criptográficas é realizado através de uma unidade certificadora interna para o domínio corporativo, conforme descrito procedimentos internos seguidos e controlados pela equipe de suporte interno (infraestrutura de TI) da Central IT. Certificados utilizados externamente são feitos através de aquisição de certificado digital assinado e publicamente aceitos que devem sempre ser informados e previamente autorizados pela equipe Interna de TI.

5.4 Sincronização de Relógios

Todos os computadores da rede da Central IT são sincronizados com um servidor de hora centralizado que ajusta o horário das estações sempre que ocorre a autenticação de entrada do usuário.
É responsabilidade do suporte interno da Central IT, tomar as devidas providências para manter os sistemas de processamento da informação com a hora configurada de acordo com o servidor central de hora.

6 GLOSSÁRIO

Segurança da informação: Conjunto de medidas técnicas, administrativas e organizacionais que visam proteger a confidencialidade, integridade e disponibilidade das informações.

Recursos de tecnologia da informação: Recursos de tecnologia da informação são os ativos que uma organização utiliza para coletar, processar, armazenar, distribuir e usar informações. Esses ativos podem ser tangíveis, como hardware, software e infraestrutura, ou intangíveis, como conhecimento, processos, entre outros;

Usuário: Pessoa que acessa ou utiliza de forma legítima e autorizada os ativos de informação de uma organização.

Autenticação: Processo de verificação da identidade de um usuário ou dispositivo.

Autorização: Processo de concessão de acesso a recursos ou sistemas a um usuário ou dispositivo.

Confidencialidade: Propriedade de uma informação que deve ser mantida oculta de pessoas não autorizadas.

Disponibilidade: Propriedade de uma informação ou sistema que deve estar disponível para uso quando necessário.

Integridade: Propriedade de uma informação que deve estar completa e precisa.

Mídias de armazenamento: Dispositivos físicos que armazenam dados, como discos rígidos, pendrives e CDs.

Risco: Probabilidade de um evento negativo ocorrer e seu impacto potencial.

Classificação da informação: Processo de categorização das informações de acordo com seu nível de confidencialidade, integridade e disponibilidade.

Dispositivo móvel: Uso de dispositivos móveis, como laptops, tablets e smartphones, para acessar e processar informações.

Encarregado pelo tratamento de dados pessoais: Pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Operador: Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Titular: Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Incidentes de segurança: Eventos que podem comprometer a segurança da informação, como acessos não autorizados, vazamentos de dados e ataques cibernéticos.

Política de senha: Conjunto de regras que definem os requisitos para a criação e uso de senhas.

Teletrabalho: Trabalho realizado fora das instalações da empresa, geralmente utilizando tecnologias de comunicação e informação.